User's Guide

InRow RC/RD/RP (600mm)

ACRC500
ACRC501
ACRD500
ACRD501
ACRP100
ACRP101
ACRP500
ACRP501

Contents

Introduction

Product Description

Features of the InRow RC/RD/RP (600 mm) cooling unit

The American Power Conversion (APC®) InRow RC/RD/RP (600 mm) cooling unit is a modular air conditioning unit that is available in either a direct expansion (DX) model (ACRD500 series or ACRP100 series) or a chilled water (CW) model (ACRC500 series or ACRP500 series). It is the width of a standard enclosure (600 mm), and can be placed in a data-center row. It provides full management capabilities over a network using HyperText Transfer Protocol (HTTP), Telnet, HTTP over Secure Sockets Layer (HTTPS), Secure Shell (SSH), Simple Network Management Protocol (SNMP), File Transfer Protocol, (FTP), Secure CoPy (SCP), and Modbus. The cooling unit provides the following features:

- Group control
- Temperature monitoring
- Remote shutdown
- Output contact monitoring
- Event log accessible by Telnet, FTP, SSH, SCP, serial connection, the display interface, or a Web browser
- SNMP traps and e-mail notifications sent in response to events
- Syslog events sent to configured Syslog servers
- Security protocols for authentication and encryption

Initial setup

You must define the following three TCP/IP settings for the cooling unit before it can operate on the network:

- IP address of the cooling unit
- Subnet mask
- IP address of the default gateway

Note: Never use the loopback address (127.0.0.1) as the default gateway address for the cooling unit. Doing so will disable the unit and will require you to reset TCP/IP settings to their defaults using a local serial login.

To use a DHCP server to configure the TCP/IP settings for a cooling unit, see “TCP/IP settings” on page 37.

To configure the TCP/IP settings, see the *Installation Manual* for your cooling unit, provided in printed form and in PDF on either the *Utility* CD or on the APC Web site, **www.apc.com**.

Internal Management Features

Overview

You can manage the cooling unit through the Web interface, display interface, control console, Modbus, or SNMP. SNMP requires the PowerNet® MIB, available on the *Utility* CD or from the APC Web site, **www.apc.com**.

For more information about the menu-driven interfaces of the cooling unit, see “Web Interface” on page 13 and “Control Console” on page 6.

For more information about the display interface, see the *Operation and Maintenance* manual for your cooling unit, available on the *Utility* CD or on the APC Web site, **www.apc.com.**

To download the latest version of the Modbus register map, go to the APC Web site, **www.apc.com**, search by part number, and click the link to the register map in the list of documentation. Check the publication date at the start of the file.
For more information about Modbus, see the Modbus Standard Library at **www.modbus.org**.

To use the PowerNet MIB with an SNMP browser, see the *PowerNet SNMP Management Information Base (MIB) Reference Guide*, provided on the *Utility* CD.

Access priority for logging on

Only one user at a time can log on to the cooling unit to use its internal user interface features. The priority for access is as follows:

- Local access to the control console from a computer with a direct serial connection to the cooling unit always has the highest priority.
- Telnet or Secure SHell (SSH) access to the control console from a remote computer has the next highest priority.
- Web access, either directly or through the InfraStruXure Central, has the lowest priority.

For information on how to control SNMP access to the cooling unit, see “SNMP” on page 46.

Types of user accounts

The cooling unit has three levels of access (Administrator, Device User, and Read-Only User), all of which are protected by user name and password requirements.

- An Administrator can use all of the management menus available in the control console and the Web interface. The Administrator's default user name and password are both **apc**.
- A Device User (Device Manager in the control console) can access only the **Log** option in the **Events** menu and use the **Group**, **Unit**, and **Alarms** menus. The Device User's default user name is **device**, and the default password is **apc**.
- A Read-Only User has the following restricted access:
  - Access through the Web interface only.
  - Access to the same menus as a Device User, but without the capability to change configurations, control devices, or delete data. Links to configuration options may be visible but are disabled, and the event log displays no **Clear Log** button.
  - The Read-Only User's default user name is **readonly**, and the default password is **apc**.

To set **User Name** and **Password** values for the Administrator, Device User, and Read-Only User accounts, see "Setting user access" on page 32. You must use the Web interface to configure values for the Read-Only User.

How to Recover from a Lost Password

Use a local computer, a computer that connects to the cooling unit through the serial port, to access the control console.

1. Select a serial port at the local computer and disable any service that uses that port.
2. Connect the configuration cable (APC part number 940-0103 and extension, if required, 940-1000A) to the selected port on the computer and to the serial port at the cooling unit (use the DB-9 connector on the front of the electrical panel).

   Note: Do not touch components on the electrical panel, other than the service port.

3. Run a terminal program (such as HyperTerminal) and configure the selected port as follows:
   - 9600 bps
   - 8 data bits
   - no parity
   - 1 stop bit
   - no flow control
4. Press ENTER on the computer, repeatedly if necessary, to display the **User Name** prompt.
5. If you are unable to display the **User Name** prompt, verify the following:

   – The serial port is not in use by another application.

   – The terminal settings are correct as specified in step 3.

   – The correct cable is being used as specified in step 2.
6. Switch the main breaker to OFF. Wait one second. Switch the main breaker to ON.

   Note: If you wait too long to return power to the cooling unit, you must repeat step 5.

7. Press ENTER as many times as necessary to redisplay the **User Name** prompt, then use the default, **apc,** for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must repeat step 5 and log on again.)
8. From the **Control Console** menu, select **System**, then **User Manager**.
9. Select **Administrator**, and change the **User Name** and **Password** settings, both of which are now defined as **apc**. Select **Accept Changes** to store the new user name and password values.
10. Press CTRL+C, log off, reconnect any serial cable you disconnected, restart any service you disabled.

Display Interface LEDs

Status

This LED indicates the status of the cooling unit.

Condition	Description
Off	The cooling unit has no power.
Solid Green	The cooling unit is receiving power.
Flashing Green	The cooling unit is receiving a firmware upgrade.

Check log

When yellow, this LED indicates that at least one new critical alarm, warning alarm, or event has occurred since the last time the event log was viewed from the display interface.

Warning alarm

When yellow, this LED indicates that a warning alarm condition exists and may require your attention to prevent it from deteriorating into a critical state. A new alarm will cause a beep every 30 seconds until you silence the alarm by pressing any function key.

Critical alarm

When red, this LED indicates that a critical alarm condition exists and requires your immediate attention. An audible alarm beeps every 30 seconds. Press any function key to silence the audible alarm.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the cooling unit uses internal, system-wide watchdog mechanisms. When it reboots to recover from an internal problem, a **System: Warmstart** event is recorded in the event log.

Network interface watchdog mechanism

The cooling unit implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the cooling unit does not receive any network traffic for 9.5 minutes (either direct traffic, such as SNMP, or broadcast traffic, such as an Address Resolution Protocol [ARP] request), it assumes that there is a problem with its network interface and restarts.

Resetting the network timer

To ensure that the cooling unit does not restart if the network is quiet for 9.5 minutes, the cooling unit attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the cooling unit, and that response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network most of the time and is on the same subnet. The network traffic of that computer will reset the 9.5-minute timer frequently enough to prevent the cooling unit from restarting.

Control Console

How to Log On

Overview

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection to access the control console.

Use case-sensitive user name and password entries to log on (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device User). A Read-Only User cannot access the control console.

If you cannot remember your user name or password, see “How to Recover from a Lost Password” on page 4.

Remote access to the control console

You can access the control console through Telnet or Secure SHell (SSH), depending on which is enabled. (An Administrator can enable these access methods through the **Telnet/SSH** option of the **Network** menu.) By default, Telnet is enabled. Enabling SSH automatically disables Telnet.

Telnet for basic access. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption. To use Telnet to access the control console from any computer on the same subnet:

1. At a command prompt, type `telnet` and the System IP address for the cooling unit (when the cooling unit uses the default Telnet port of 23), and press ENTER. For example:

   ```
   telnet 139.225.6.133
   ```

   Note: If the cooling unit uses a non-default port number (between 5000 and 32767), you need to include a colon or a space (depending on your Telnet client) between the IP address and the port number.

2. Enter the user name and password (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device User).

SSH for high-security access. If you use the high security of SSL for the Web interface, use Secure SHell (SSH) for access to the control console. SSH encrypts user names, passwords, and transmitted data.

The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet, but to use SSH, you must first configure SSH and have a SSH client program installed on your computer.

Local access to the control console

You can use a local computer that connects to the cooling unit through the serial port.

Note: To access the serial port, remove the front panel and lower air filter of the cooling unit.

1. Select a serial port at the local computer and disable any service that uses that port.
2. Use the configuration cable (APC part number 940-0103 and extension, if required, 940-1000A) to connect the selected port of the local computer to the serial port at the cooling unit (use the DB-9 connector on the front of the electrical panel).
3. Run a terminal program (such as HyperTerminal) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
4. Enter the user name and password for the access desired (Administrator or Device User).

Main Screen

Example main screen

The following is an example of the screen that appears when you log on to the control console at the cooling unit.

```
User Name : apc
Password  : ***


American Power Conversion          Network Management Card AOS   vx.x.x
Copyright 2005 All Rights Reserved   InRow RC                  APP    vx.x.x
--------------------------------------------------------------------------------
Name:       InRow RC                                      Date : 04/29/2009
Contact:    Bill Cooper                                   Time : 10:16:58
Location:   Testing Lab                                   User : Administrator
Up Time:    0 Days 0 Hours 43 Minutes                     Stat : P+ N+ A+

Cooling Group Status : None
Cooling Unit  Status : None

------- Control Console --------------------------------------------------------

     1- Device Manager
     2- Network
     3- System
     4- Logout

<ESC>- Main Menu, <ENTER>- Refresh, <CTRL-L>- Event Log
```

Information and status fields

Main screen information fields.

Two fields identify the APC operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the type of device that connects to the network. On the example main screen, the application firmware for the cooling unit is displayed.

```
Network Management Card AOS                    vx.x.x

InRow RC APP                                   vx.x.x
```

- Three fields identify the system **Name**, **Contact**, and **Location** values.

  ```
  Name:          InRow RC
  Contact:       Bill Cooper
  Location:      Testing Lab
  ```

  To set the **Name**, **Contact**, and **Location** values, see “Identification” on page 21.

- An **Up Time** field reports how long the management interface has been running since it was last reset or since power was applied.

  ```
  Up Time: 0 Days 0 Hours 43 Minutes
  ```

- Two fields identify the date and time at which the screen most recently refreshed.

  ```
  Date: 03/29/2009
  Time: 10:16:58
  ```

- A **User** field identifies whether you logged on as Administrator or Device User.

  ```
  User: Administrator
  ```

  or

  ```
  User: Device Manager
  ```

Main screen status fields.

- A **Stat** field reports the cooling unit status.

  ```
  Stat: P+ N+ A+
  ```

`P+`	The APC operating system (AOS) is functioning properly.
`N+`	The network is functioning properly.
`N?`	A BOOTP or DHCP request cycle is in progress.
`N-`	The cooling unit failed to connect to the network.
`N!`	Another device is using the IP address of the cooling unit.
`A+`	The application is functioning properly.
`A-`	The application has a bad checksum.
`A?`	The application is initializing.
`A!`	The application is not compatible with the AOS.

Note: If the AOS status is not P+, contact “APC Worldwide Customer Support” at the web address on the back cover, even if you can still access the cooling unit.

Cooling unit status field. The **Status** field displays the status of the cooling units. Under normal operation this field will read:

```
Cooling Group Status: None

Cooling Unit  Status: None
```

`None` will be replaced with `Warning` or `Critical` if an alarm condition exists.

Control Console Menus

Menu structure

The menus in the control console list options by number and name. To use an option, type the option's number and press ENTER, then follow any on-screen instructions.

For menus that allow you to change a setting you must use the **Accept Changes** option to save the changes you made. Some changes may only take effect after you log off.

While in a menu, you can also do the following:

- Type `?` and press ENTER to access a brief menu of option descriptions (if the menu has help available).
- Press ENTER to refresh the menu.
- Press ESC to return to the menu from which you accessed the current menu.
- Press CTRL+C to return to the main (control console) menu.
- Press CTRL+L to access the event log.

For more information about the event log, see "Events" on page 24.

Main menu

The main control console menu has options that provide access to the management features of the control console.

`1- Device Manager` (equivalent to Device User in the Web interface)
`2- Network`
`3- System`
`4- Logout`

Note: When you log on as Device Manager, you do not have access to the **Network** or **System** menus.

Device Manager option

This option accesses the **Device Manager** menu, which displays information about the unit and the group. Select the components you want to manage. For example:

```
1- View Active Alarms
2- Cooling Group
3- Cooling Unit
```

Network option

Use this option to perform any of the following tasks:

- Configure the cooling unit's TCP/IP settings.
- Configure the settings for the type of server (DHCP or BOOTP) used to provide the TCP/IP settings to the cooling unit.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet/SSH, Web/SSL, SNMP, Syslog, Serial Modbus, E-mail, and DNS features of the cooling unit.

System option

Use this option to perform any of the following tasks:

- Control **Administrator** and **Device Manager** access.
- Define the System **Name**, **Contact**, and **Location** values.
- Set the date and time used by the cooling unit.
- Restart the cooling unit's management interface.
- Reset control console settings to their default values.
- Define RADIUS access and set primary and secondary servers.

Web Interface

How to Log On

Overview

You can use the cooling unit's DNS name or System IP address for the URL address of the Web interface. Use your case-sensitive **User Name** and **Password** settings to log on. The default user name differs by account type:

- **apc** for an Administrator
- **device** for a Device User
- **readonly** for a Read-Only User

The default password is **apc** for all three account types.

Note: If you are using HTTPS as your access protocol, your login credentials are compared with information in a server certificate. If the certificate was created with the APC Security Wizard, and an IP address was specified as the common name in the certificate, you must use an IP address to log on to the cooling unit. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

For information about the Web page that appears when you log on to the Web interface, see "Summary Page" on page 15.

Supported Web browsers

You can use Microsoft® Internet Explorer (IE) 7.x and higher (on Windows operating systems only), Firefox, version 3.0.6, and higher by Mozilla Corporation (on all operating systems) to access the cooling unit through its Web interface. Other commonly available browsers also may work but have not been fully tested by APC.

Note: For optimal functioning of the Web interface, enable JavaScript® for your Web browser.

In addition, the cooling unit's management interface cannot work with a proxy server. Therefore, before you can use a Web browser to access the cooling unit's Web interface, you must do one of the following:

- Configure the Web browser to disable the use of a proxy server for the cooling unit.
- Configure the proxy server so that it does not proxy the specific IP address of the cooling unit.

URL address formats

Type the DNS name or IP address of the cooling unit in the Web browser's URL address field, and press ENTER. When you specify a non-default Web server port in Internet Explorer, you must include `http://` or `https://` in the URL.

Common browser error messages at log on

Error Message	Browser	Cause of the Error
“You are not authorized to view this page” or “Someone is currently logged in...”	Internet Explorer, Firefox	Someone else is logged on.
“This page cannot be displayed.”	Internet Explorer	Web access is disabled, or the URL was not correct
“Unable to connect.”	Firefox	

- For a DNS name of Web1, the entry would be one of the following:
  – `http://Web1` if HTTP is your access mode
  – `https://Web1` if HTTPS is your access mode
- For a System IP address of 139.225.6.133, when the cooling unit uses the default port (80) at the Web server, the entry would be one of the following:
  – `http://139.225.6.133` if HTTP is your access mode
  – `https//139.225.6.133` if HTTPS is your access mode
- For a System IP address of 139.225.6.133, when the cooling unit uses a non-default port (5000, in this example) at the Web server, the entry would be one of the following:
  – `http://139.225.6.133:5000` if HTTP is your access mode
  – `https://139.225.6.133:5000` if HTTPS is your access mode

Summary Page

When you log on to the Web interface at the cooling unit, navigation tabs are displayed at the top of the screen. Below the navigation tabs, a top menu bar lists options related to the selected tab. The status field displays information about the selected tab or top menu bar option.

Navigation tabs

Five tabs are displayed at the top of the screen:

- **Home**—View any active alarm or warning conditions and clear active alarms; this tab is displayed when you log on for the first time.
- **Group**—View and configure group settings.
- **Unit**—View cooling settings, unit properties, identification information, view or reset run hours, and configure service intervals.
- **Logs—**View and configure the event and data logs, and configure Syslog settings.
- **Administration—**Configure security, network connection, notification, and device settings.

Quick status

The quick status tab is displayed in the upper right of every screen in the Web interface. The tab displays a warning of any alarms.

✓	Click the green "device operating normally" icon to return to the status screen where the status of the cooling unit is displayed.
⚠	Click the "attention required" icon to return to the status screen where active warnings and alarms are displayed.
✖	Click the "alarm detected" icon to return to the status screen where active alarms are displayed.

Status

The Active Alarms field displays the states (No alarms present, Warning, or Critical) of both the cooling group and individual cooling units. The Recent Device Events table displays the five most recent device events, and the dates and times they took place. Click **More Events** at the bottom of the Recent Device Events table to see the entire event log.

Help

Click **Help**, located in the upper right hand corner of the Web interface, to view context-sensitive information.

Select a tab to perform a task

To do the following, see “Home” on page 18:

- View and clear alarms.

To do the following, see “Group” on page 18:

- View the status of the group.
- Set the number of units in the group.
- Define the configuration type used by the group.
- Set the cool setpoints. For the ACRP100 series and ACRP500 series only, set the humidify, dehumidify, and reheat setpoints.
- Set the fan speed preference.
- Set the cool, dehumidify, and reheat PIDs, and the humidify sensitivity band (ACRP100 series and ACRP500 series only).
- Set the percentage of glycol in the group (ACRC500 series and ACRP500 series).

To do the following, see “Unit” on page 20:

- View the status and properties of each unit.
- Set unit delays.
- Change the unit identification values.
- Configure and control the modes.
- Assign the type of alarm that will activate the output sensor.
- Set the normal state of the input and output.
- Reset the unit run hours alarms.
- Set alarm threshold values.
- Set service intervals.

To do the following, see “Logs” on page 24:

- Access the event and data logs.
- Set the interval and rotation for the data log.
- Create data log graphs.
- Configure Syslog settings.

To do the following, see “Administration: Security” on page 32:

- Control Administrator, Device User, and Read-Only user access.
- Configure RADIUS access, servers, and server secret.

To do the following, see “Administration: Network” on page 37:

- Configure new TCP/IP settings for the cooling unit.
- Select the port speed.
- Identify the Domain Name System (DNS) Server and test the network connection to that server.
- Define settings for the FTP server, SNMP, Control Console/SSH, and Web/SSL.

To do the following, see “Administration: Notification” .

- Configure the actions to be taken based on an event’s severity level.
- Configure SNMP Trap Receiver settings for sending event-based traps.
- Define who will receive e-mail notifications of events.
- Test e-mail settings.

To do the following, see “Administration: General Options” on page 55:

- Define the System name, contact, and location values.
- Set the date and time used by the cooling unit.
- Select the temperature scale used by the cooling unit.
- Restart the user interface of the cooling unit.
- Reset network interface settings to their default settings.
- Upload a user configuration file.
- Configure Modbus settings.
- View information about the cooling unit.
- Define the URL addresses of the user links in the Web interface.

Cooling Unit Operation

Home

Overview

View a summary of the following:

- Active alarms
- Group status
- Unit status
- Recent device events

Alarm status

View the following alarm information:

- Group alarm status showing alarm descriptions and severity level
- Unit alarm status showing alarm descriptions and severity level

You can also choose to clear active alarms.

Group

Overview

View the following properties that are group-level or common to each unit in the group:

- Cool setpoint—in degrees Celsius (C) or Fahrenheit (F)
- Air flow—in cubic feet per minute (CFM) or liters per second (L/s)
- Maximum rack inlet temperature
- Minimum rack inlet temperature
- Cool output—in kilowatts (kW)
- Cool demand—in kW
- Humidify, Dehumidify and Reheat output — as a percentage of full output (ACRP100 and ACRP500 cooling units only)
- Humidify, Dehumidify and Reheat demand — as a percentage of full demand (ACRP100 and ACRP500 cooling units only)

Setpoints

Assign the following group setpoints and then click **Apply**. The setpoints for each mode must be within the following ranges:

- **Cool**: 64.4–77.0°F (18.0–25.0°C)
- **Supply Air**: 62.6–73.4°F (17.0–23.0°C)

The following setpoints apply to the ACRP100 and ACRP500 cooling units:

- **Dehumidify**: 35.0–60.0% RH
- **Dehumid Deadband**: 2.0–10.0%
- **Humidify**: 25.0–50.0% RH
- **Reheat**: 50.0–64.4°F (10.0–18.0°C)

For ACRP100 and ACRP500 cooling units: The **Supply Air** setpoint must be at least 2.0°F (1.1°C) above the **Reheat** setpoint. The **Dehumidify** setpoint must be at least 5% above the **Humidify** setpoint. If the **Supply Air** setpoint is greater than the **Cool** setpoint, the cooling unit activates an alarm and resets the **Supply Air** setpoint to equal the **Cool** setpoint.

Configuration

Number of units in group. Enter the number of units in the group, then click **Apply**. Up to twelve units can be configured to work as a group.

Configuration type. Select the configuration type, which is the air flow control strategy the group uses, then click **Apply**:

- **RACS**—Rack Air Containment System. Air flow in the enclosure is controlled by a ducting system fitted to the enclosure.
- **HACS**—Hot Aisle Containment System. Air flow in the room is controlled by enclosing the hot air aisle.
- **In-Row**—Air flow is horizontal, to allow in-row operation of the cooling group.

Percent glycol. Enter the percentage of glycol the group uses to cool the environment. This information is used to calculate the amount of energy (in kW) required by the unit. **Percent glycol** applies only to ACRC500 and ACRP500 cooling units. Only a qualified service technician should change the amount of glycol in the group.

PID control settings. For ACRP100 and ACRP500 cooling units. The Proportional + Integral + Derivative (PID) control loop is used to control the output of the group. Enter the settings for the **Cool** and **Reheat PID**s, and the **Humidify Sensitivity Band,** then click **Apply**.

Note: The loops must be tuned after the room load is in place, and then periodically if the room load changes. Only a qualified service technician should perform PID tuning.

For more information about PID tuning, see the *Operation and Maintenance* manual for your cooling unit, available on the *Utility* CD or on the APC Web site, **www.apc.com.**

Unit

Overview

View information for the various components of each unit in the group, including the following:

- Operating mode—On, Standby, or Idle
- Maximum Rack Inlet—in degrees F or C
- Supply and Return Air Temperatures—in degrees F or C
- Supply and Return Humidity—in percent relative humidity
- Air flow—in CFM or L/s
- Fan speed—the average RPM of all fans, given as a percentage of the maximum fan speed
- Cool output and demand—in kW
- Humidify, Dehumidify, and Reheat (ACRP100 and ACRP500 series only) output and demand—as a percentage of full output and demand

Detailed status

View information for the components of the units in the group:

- Input and output contact states — open or closed.
- Active power source (ACRC500 and ACRP500 cooling units only) — the power source supplying power to the unit, A or B.
- Rack inlet sensors — the temperature of the air at the sensors.
- Filter differential pressure — the difference in pressure on either side of the air filter.
- Containment differential pressure — RACS or HACS configurations only. The difference in pressure between the front of the unit and the rear of the unit. This value affects fan speed control.
- Humidifier current (ACRP100 and ACRP500 cooling units only) — the current draw from the humidifier canister.
- Humidifier water conductivity (ACRP100 and ACRP500 cooling units only) — the conductivity of the water in the humidifier canister.
- Suction pressure (ACRD500 and ACRP100 cooling units only) — the pressure at the compressor inlet.
- Discharge pressure (ACRD500 and ACRP100 cooling units only) — the pressure at the compressor outlet.
- Fluid valve position (ACRC500 and ACRP500 cooling units only) — how much the valve is opened, as a percentage of the fully open position .
- Fluid flow (ACRC500 and ACRP500 cooling units only) — the volume of fluid that is flowing through the unit.
- Entering and leaving fluid temperature (ACRC500 and ACRP500 cooling units only) — the temperature of the fluid as it enters and as it leaves the unit.

Compressor drive status (ACRD500 and ACRP100 cooling units)

View the following information about each cooling unit:

- Speed
- Power
- Voltage
- Current
- DC Link Voltage
- Heat Sink Temperature
- Control Card Temperature
- Warning Status
- Alarm Status

Identification

The **Unit** tab's left navigation menu option **Identification** displays the following read-only information about each unit:

- Model Number
- Serial Number
- Controller Firmware
- Hardware Revision
- Date of Manufacture

You can also configure the following identification information:

- **Unit ID**—Assign the unit a number from 1 to 12. The **Unit ID** must be unique for each cooling unit within the cooling group.
- **Name**—Enter a name (up to 20 alphanumeric characters) for the unit.
- **Location—**Enter the location (up to 20 alphanumeric characters) of the unit.

Click **Apply** to save your changes.

Run hours

View the run hours of the unit components. To reset the run hours, select the unit components to set to zero and click **Apply**.

Service intervals

Set the service interval for each of the components, in weeks. The default are:

- **Air Filter**—18 weeks
- **Humidifier**—26 weeks
- **Heater**—52 weeks
- **Condensate Pump**—52 weeks
- **Fans**—52 weeks
- **Compressor** (ACRD500 series and ACRP100 series only)—52 weeks

Enable or disable alarm generation for the service intervals for each of the unit components, then click **Apply** to save your changes.

Thresholds

For ACRC500 and ACRP500 cooling units, configure high temperature thresholds for the rack inlet, supply air, return air, and entering fluid temperature sensors. Valid values are 0° to 37.2°C (32° to 99°F) for the entering fluid temperature sensors, and 0° to 100°C (32° to 212°F) for the rack inlet, supply air, and return air sensors.

For ACRP100 and ACRP500 cooling units, configure thresholds for supply high humidity and supply low humidity. Valid values are 0% to 100% relative humidity.
Click **Apply** to save your changes.

Sensor Values:

- **Rack Inlet Temperature** — 68.5°F
- **Supply Air Temperature** — 68.7°F
- **Return Air Temperature** — 69.2°F
- **Supply Humidity** — 29.3% RH
- **Return Humidity** — 32.4% RDH

Thresholds:

- **Rack Inlet High Temperature** — 32.0 - 212.0 °F
- **Supply Air Temperature** — 32.0 - 212.0 °F
- **Return Air Temperature** — 32.0 - 212.0 °F
- **Supply Humidity** — 35.0 - 90.0 % RH
- **Return Humidity** — 20.0 - 50.0 % RDH

Configuration

Configure the following unit settings, then click **Apply** to save your changes:

- **Startup Delay** — The delay that begins when power is applied. The unit starts when the delay period ends. This allows you to create a staged restart after a power loss. Valid values are 0 to 999 seconds.
- **Cool Capacity** (ACRC500 and ACRP500 cooling units only) — The setting used to determine chilled water flow to the unit. Use **Automatic** to have the cooling unit automatically control its output under normal (default) conditions. Use **Maximum** to run the cooling unit at full capacity. For ACRP500 cooling units only: Heating, Humidifying, and Dehumidifying are disabled in **Maximum** mode.
- **Idle on Leak Detect** — When enabled, this setting causes the unit to idle when a leak is detected; the default setting is **No**.
- **Input Normal State** — The normal state for the input contact, open or closed. When the input is not in its normal state, the unit will stop cooling.
- **Output Normal State** — The normal state for the output relay, open or closed.
- **Output Source** — The type of alarm that will activate the output relay, any alarm, or only critical alarms.
- **Humidify** (ACRP100 and ACRP500 cooling units only) — Enable or disable the humidify function.
- **Humidifier control** (ACRP100 and ACRP500 cooling units only) — Select **Auto** to have the main controller control the humidifier. Select **Drain/Off** to drain the humidifier and then turn it off.
- **Dehumidify** (ACRP100 and ACRP500 cooling units only) — Enable or disable the dehumidify function.
- **Reheat** (ACRP100 and ACRP500 cooling units only) — Enable or disable the reheat function.
- **Display Units** — The units (metric or US) displayed for each cooling unit.

Logs

Events

Log

Use this option to view or delete the contents of the event log. The event log displays all events recorded since the log was last deleted or since the log reached its maximum capacity and the older half was deleted automatically. Events are listed in reverse chronological order. By default, all events are logged:

- You can view the event log as a page of the Web interface (the default view) or click **Launch Log in New Window** from that page to display a full-screen view of the log, enabling you to see more of the listed events without scrolling.

  Note: If your browser is Microsoft Internet Explorer, JavaScript must be enabled for you to use the **Launch Log in New Window** button.

  Alternatively, you can use FTP or Secure CoPy (SCP) to view the event log. See "How to use FTP or SCP to retrieve the log files" on page 30.

- To delete all events recorded in the log, click **Clear Event Log** on the Web page that displays the log. Deleted events cannot be retrieved.

To disable the logging of events based on their assigned severity level or their event category, configure event actions by group.

See "Configuring by group" on page 51.

To access lists of all configurable events and how they are currently configured, select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu; then click, in turn, on each major category of event.

See "Configuring by event" on page 49.

Reverse lookup

Reverse lookup is disabled by default. Enable this feature unless you have no DNS server configured or have poor network performance because of heavy network traffic.

With reverse lookup enabled, when a network-related event occurs, both the IP address and the domain name for the networked device associated with the event are logged in the event log. If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change much less frequently than IP addresses, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events to occur.

Data

Log

Use this option to access a log that periodically records cooling unit data. Each entry is listed by the date and time the data was recorded and provides the data in a column format.

To view the data log through the Web interface, click **log**.

Click **Launch Log in New Window** to launch the data log in a new browser window that provides a full-screen view.

Note: If your browser is Microsoft Internet Explorer, JavaScript must be enabled for you to use the **Launch Log in New Window** button.

Alternatively, you can use FTP or Secure CoPy (SCP) to view the data log. See "How to use FTP or SCP to retrieve the log files" on page 30.

Click **Clear Data Log** to delete all data recorded in the log. Deleted data cannot be retrieved.

Graphing

Use this option to create an interactive data graph. Select a maximum of four data parameters from the **Graph Data** pull down menu. Choose a time frame from the **Graph Time** pull down menu or enter a date range in the **From** and **To** fields. Click **Apply** to generate the graph.

Click **Launch Graph in New Window** to launch the graph in a new browser window that provides a full-screen view.

Use the zoom tool above the graph to magnify the data shown on the screen. You can also click on any point in the graph to center and magnify that point on the screen. Use the left or right arrow bar to navigate through the data displayed in the magnified graph. Hover over any horizontal line in the graph to view the date, time, and Y-axis value for that data record.

Interval

Use this option to define, in the **Log Interval** setting, how frequently data is sampled and stored in the data log. This Web interface page also reports how many days of data the log can store, based on the interval you selected.

When the log is full, the older half of the log is deleted and the newer half is retained. To avoid automatic deletion of older data, enable and configure data log rotation as described in the next section.

Rotation

Use this option to set up a password-protected data log repository on a specified FTP server. Enabling rotation causes a copy of any previously unsaved entries in the data log to be appended to the file you specify by name and location. Updates to this file occur either at the upload interval that you specify, in hours, or when the data log has reached its maximum size (if the maximum size is reached before the upload interval expires).

Parameter	**Description**
Last Upload Result	Indicates whether the last upload of the data file to the FTP server succeeded or failed, or displays "None Available."
Data Log Rotation	Enable or disable (the default) data log rotation.
FTP Server	The location (IP address or host name) of the FTP server where the data repository file is stored.
User Name	The user name required to send data to the repository file. This user must also be configured to have read and write access to the data repository file and the directory (folder) in which it is stored.
Password	The password required to send data to the repository file.
File Path	The path to the repository file.
File Name	The name of the repository ASCII text file.
Delay *hours* between Uploads	The number of hours between uploads of data to the specified file.
Retry Delay	The time that the system waits before retrying an upload after a failed attempt. You can specify that the upload will be retried repeatedly until it succeeds or you can limit the number of retries. If you specify a limited number of retries and the upload has been retried unsuccessfully the specified number of times (**Number of Retries**), the scheduled upload is skipped, and the system waits the number of hours specified as **Delay *hours* between Uploads**.
Number of Retries	The number of times the upload will be attempted after an initial failure.

To initiate the initial upload of data to the repository file immediately, click **Upload Now!**

Syslog

By default, the cooling unit can send messages to up to four Syslog servers whenever events occur. The Syslog servers, which must be specifically identified by their IP addresses or host names, record the events that occur at network devices in a log that provides a centralized record of events.

This user's guide does not describe Syslog or its configuration values in detail. For more information about Syslog, see RFC3164, at **www.ietf.org/rfc/rfc3164.txt?number=3164**.

Servers

Use this option to identify one or more Syslog servers that will receive Syslog messages and to specify a port for each. Select the server address to edit existing server configurations or select **Add Server** to configure additional servers.

Setting	Definition
Syslog Server	Uses specific IP addresses or host names to identify up to four servers that will receive Syslog messages sent by the cooling unit. **Note:** To use the Syslog feature, **Syslog Server** must be defined for at least one server.
Port	Identifies the user datagram protocol (UDP) port that the cooling unit will use to send Syslog messages. The default is **514**, the number of the UDP port assigned to Syslog.

Settings

Leave the Syslog settings, except the **Server IP** settings, set to their defaults unless otherwise specified by the Syslog network or system administrator.

Setting	Definition
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the cooling unit's Syslog messages (**User**, by default). **Note: User** is the selection that best defines the Syslog messages sent by the cooling unit. Do not change this selection unless advised to do so by the Syslog network or system administrator.
Severity Mapping	Maps each of the severity levels assigned to cooling unit events to the available Syslog priorities. You should not need to change the default mappings. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the four **Local Priority** settings: • **Critical** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** **Note:** To disable sending Syslog messages for **Critical**, **Warning**, or **Informational** events, see "Configuring event actions" on page 49.

Test

Use this option to send a test message to the Syslog servers configured through the **servers** option:

1. Select a severity to assign to the test message.
2. Define the test message, using any text that is formatted according to the required message (MSG) fields. The message fields, which you format, are one of the three parts of the Syslog message that will be sent. For example, `APC: Test Syslog`, meets the formatting requirements.
   - The priority (PRI) identifies the Syslog priority assigned to the message's event and the facility code assigned to messages sent by the cooling unit.
   - The Header includes a time stamp and the IP address of the cooling unit.
   - The message (MSG) part has two fields:
     - A TAG field, which is followed by a colon and a space, identifies the event type.
     - A CONTENT field provides the event text, followed (optionally) by a space and the event code.

How to use FTP or SCP to retrieve the log files

If you are an Administrator or Device User, you can use FTP or SCP to retrieve a tab-delineated event log file `(event.txt)` or data log file `(data.txt)` that you can import into a spreadsheet application.

- The file reports all of the events recorded since the log was last deleted.
- The file includes information that the event log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, **Location** values, and **IP address** of the cooling unit
  - The unique **Event Code** for each recorded event (event log only)

Note: The cooling unit uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits of the year.

If you are using the encryption-based security protocols for your system, use Secure CoPy (SCP) to retrieve the log file. (You should have FTP disabled.)

If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.

See the *Security Handbook*, available on the *Utility* CD and on the APC Web site (**www.apc.com**) for information on the available protocols and methods for setting up the type of security appropriate for your needs.

To use SCP to retrieve the file. To use SCP to retrieve the `event.txt` file, use the following command:

```
scp username@hostname_or_ip_address:event.txt./event.txt
```

To use SCP to retrieve the data.txt file, use the following command:

```
scp username@hostname_or_ip_address:data.txt./data.txt
```

To use FTP to retrieve the file. To use FTP to retrieve the *event.txt* or *data.txt* file:

1. At a command prompt, type `ftp` and the Management Card's IP address, and press ENTER. If the **Port** setting for the **FTP Server** option (which you select on the **Network** menu of the **Administration** tab) has been changed from its default value (**21**), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

   ```
   ftp>open ip_address port_number
   ```

   To set a non-default port value to enhance security for the FTP Server, see "FTP server" on page 48. You can specify any port from 5001 to 32768.

1. Use the case-sensitive **User Name** and **Password** for either an Administrator or a Device User to log on.

   - For Administrator, **apc** is the default for **User Name** and **Password**.
   - For the Device User, **device** is the default for **User Name**, and **apc** is the default for **Password**.

2. Use the **get** command to transmit the text-version of the event log or data log to your local drive.

   ```
   ftp>get event.txt
   ```

   or

   ```
   ftp>get data.txt
   ```

3. You can use the **del** command to clear the contents of the event log or data log.

   ```
   ftp>del event.txt
   ```

   or

   ```
   ftp>del data.txt
   ```

   You will not be asked to confirm the deletion. If you clear the event log, a new *event.txt* file is created to record the event.

4. Type `quit` at the `ftp>` prompt to exit from FTP.

Queries (Modbus requests and SNMP GETs)

See "About" on page 58 for information on configuring and using the request/response structure of building management systems using the Modbus protocol, and see "access control" on page 46, under "SNMP" for a description of SNMP access types that enable an NMS to perform informational queries. Configuring the most restrictive SNMPv1 access type, READ, enables informational queries without the risk of allowing remote configuration changes.

Administration: Security

Local Users

Permission levels

Before you configure user access, be sure you understand the capabilities of each account type (Administrator, Device User, and Read-Only User) to use menus, view information, and change settings.

For information on user permission levels for each account type (Administrator, Device User, and Read-Only User), see “Types of user accounts” on page 3.

Setting user access

You set the user name and password for each of the account types in the same manner.

User name. The case-sensitive user name (maximum of 10 characters) is used by Administrators and Device Users to log on at the control console, display interface, or Web interface and by the Read-Only User to log on at the Web interface. Default values are **apc** for Administrator, **device** for Device Users, and **readonly** for the Read-Only User.

Password. The case-sensitive password (maximum of 10 characters) is used to log on to the Web interface, (except for the Read-Only User) the control console, or the display interface. The default setting for **Password** is **apc** for Administrators, Device Users, and Read-Only Users.

Remote Users

Authentication

Use this option to select how to administer remote access to the cooling unit:

For information about local authentication (authentication that can be administered without the centralized authentication provided by a RADIUS server), see the *Security Handbook* provided on the *Utility* CD and available on the APC Web site at **www.apc.com**.

Note: APC supports the authentication and authorization functions of RADIUS (Remote Authentication Dial-In User Service).

- When a user accesses the cooling unit that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user's permission level.
- RADIUS user names used with the cooling unit are limited to 32 characters.

Select one of the following:

- **Local Device Only**: RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Device**: RADIUS is enabled, and local authentication is enabled. Authentication is requested from the RADIUS server first; local authentication is used only if the RADIUS server is not available.
- **RADIUS Only**: RADIUS is enabled. Local authentication is disabled.

  Note: If **RADIUS Only** is selected, the only way to recover if the RADIUS server is unavailable, improperly identified, or improperly configured is to use a serial connection to the control console and change the **Access** setting to **Local Device Only** or **RADIUS, then Local Device**. See "Local access to the control console" on page 7 for information about how to access the serial port.

RADIUS

Use this option to do the following:

- Display a list of RADIUS servers identified as being available to the cooling unit and the time-out period for each server (the number of seconds the cooling unit will wait for a reply from the server before the request fails).
- Add a server to the list of identified RADIUS servers. Click **Add Server**, and configure the following parameters for authentication by the new server:

RADIUS Setting	Definition
RADIUS Server	The server name or IP address of the RADIUS server. **Note:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.
Secret	The shared secret between the RADIUS server and the cooling unit.
Reply Timeout	The time in seconds that the cooling unit waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password to test the RADIUS server path that you have configured.

RADIUS Setting	Definition
Skip Test and Apply	Do not test the RADIUS server path.

Configuring the RADIUS Server

You must configure your RADIUS server to work with the cooling unit. The following procedure summarizes the steps to perform.

For examples of the file entries needed to configure a RADIUS server for use with a cooling unit, see the *Security Handbook*, available on the *Utility* CD or from the APC Web site, **www.apc.com**.

Summary of the configuration procedure

1. Add the IP address of the cooling unit to the RADIUS server client list (file).

   Note: RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.

2. The users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined instead. If no Service-Type attribute is configured, the user will have read-only access (to the Web interface only).

   See your RADIUS server documentation for information about the RADIUS users file, and see the APC *Security Handbook* for an example.

3. VSAs can be used instead of the Service-Type attributes provided by your RADIUS server. This method requires a dictionary entry and a RADIUS users file. In the dictionary file, you can define the names for the ATTRIBUTE and VALUE keywords, but not the numeric values. If you change the numeric values, RADIUS authentication and authorization will not work correctly. VSAs take precedence over standard RADIUS attributes.

   For examples of the RADIUS users file with VSAs and an example of an entry in the dictionary file on the RADIUS server, see the APC *Security Handbook*.

Configuring a RADIUS server on UNIX®, with shadow passwords

If UNIX shadow password files are used (/etc/passwd) in conjunction with the RADIUS dictionary files, the following two methods can be used to authenticate users:

- If all UNIX users have administrative privileges, add the following to the RADIUS “user” file.

  ```
  DEFAULTAuth-Type = System

  APC-Service-Type = Admin
  ```

  To allow only Device Users, change the value for APC-Service-Type to `Device`.

- Add user names and attributes to the RADIUS “user” file and verify passwords against /etc/passwd. The following example is for users `bconners` and `thawk`:

  ```
  bconnersAuth-Type = System

  APC-Service-Type = Admin

  thawkAuth-Type = System

  APC-Service-Type = Device
  ```

Supported RADIUS servers

APC supports FreeRADIUS, Microsoft IAS 2003. Other commonly available RADIUS applications may work but have not been fully tested by APC.

Inactivity Timeout

Use the **Auto Log Off** option to configure the time that the system waits before logging off an inactive user. Th default setting is 3 minutes. The maximum time setting is 10 minutes.

Administration: Network

TCP/IP and communication settings

TCP/IP settings

The **TCP/IP** option on the left navigation menu, selected by default when you choose **Network** on the top menu bar, displays the current TCP/IP settings of the cooling unit (the IP address, subnet mask, and default gateway) and the MAC address.

On the same page, **TCP/IP Configuration** provides the following options for how the TCP/IP settings will be configured when the cooling unit turns on, resets, or restarts: **Manual**, **BOOTP**, **DHCP**, and **DHCP & BOOTP**.

For information on DHCP and DHCP options, see **RFC2131** and **RFC2132**.

TCP/IP Setting	Description
Manual	The IP address, subnet mask, and default gateway must be configured manually. (The MAC address is not configurable.) Click **Next>>** and enter the new values.
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the cooling unit requests network assignment from any BOOTP server: • If it receives a valid response, it starts the network services. • If it finds a BOOTP server, but the request to that server fails or times out, the cooling unit stops requesting network settings until it is restarted. • By default, if previously configured network settings exist, and it receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible if a BOOTP server is no longer available. Click **Next>>** to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail to find a BOOTP server: [1] • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. • **If retries fail**: Select either **Use prior settings** (the default) or **Stop BOOTP request**.

[1] The default values for these three settings on the configuration pages generally do not need to be changed:
- **Vendor Class**: APC
- **Client ID**: The MAC address of the cooling unit, which uniquely identifies it on the local area network (LAN)
- **User Class**: The name of the application firmware module

TCP/IP Setting	Description
DHCP	At 32-second intervals, the cooling unit requests network assignment from any DHCP server. By default, the number of retries is unlimited. • If the cooling unit receives a valid response, by default it requires the APC cookie from the DHCP server in order to accept the lease and start the network services. • If the cooling unit finds a DHCP server, but the request to that server fails or times out, the cooling unit stops requesting network settings until it is restarted. • If a DHCP server responds with an invalid offer (for example, the offer does not contain the APC Cookie), the cooling unit accepts the lease from that server on the last request of the sequence and then immediately releases that lease. This prevents the DHCP server from reserving the IP address associated with its invalid offer. For more information on what a valid response requires, see “DHCP response options” on page 39. To specify values other than the defaults, click **Next>>** to access the **DHCP Configuration** page:[1] • **Require vendor specific cookie to accept DHCP Address**: To disable the requirement that the DHCP server provide the APC cookie, clearclear this check-box. • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.
DHCP and BOOTP	The default setting. The cooling unit tries to obtain its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server. If it obtains its TCP/IP settings from either server, it switches this setting from the default to **BOOTP** or **DHCP**, depending on the type of server that supplied the TCP/IP settings to the cooling unit. Click **Next>>** to access and configure the same settings that are available on the **BOOTP Configuration** and **DHCP Configuration** pages[1] and to specify that the **DHCP and BOOTP** setting be retained after either type of server provides the TCP/IP values.

[1] The default values for these three settings on the configuration pages generally do not need to be changed:
- **Vendor Class**: APC
- **Client ID**: The MAC address of the cooling unit, which uniquely identifies it on the local area network (LAN)
- **User Class**: The name of the application firmware module

DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings that the cooling unit needs to operate on a network, and other information that affects the cooling unit's operation.

Vendor specific information (option 43). The cooling unit uses this option in a DHCP response to determine whether the DHCP response is valid. This option contains up to two APC-specific options in a TAG/LEN/DATA format: the APC Cookie and the Boot Mode Transition.

- **APC cookie. Tag 1, Len 4, Data "1APC"**

  Option 43 communicates to the cooling unit that a DHCP server is configured to service the cooling unit. By default, this DHCP response option must contain the APC Cookie for the cooling unit to accept the lease.

  To disable the requirement of an APC cookie, see "DHCP" on page 38.

  Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie:

  ```
  Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
  ```

- **Boot mode transition. Tag 2, Len 1, Data 1/2**

  This option 43 setting enables or disables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**, which, by default, is disabled.

  – A data value of 1 enables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. Whenever the cooling unit reboots, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.

  – A data value of 2 disables the **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. The **TCP/IP Configuration** setting switches to **DHCP** when the cooling unit accepts the DHCP response. Whenever the cooling unit reboots, it will request its network assignment from a DHCP server only.

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie and the disable Boot Mode Transition setting:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43 0x02 0x01 0x01
```

TCP/IP options. The Management Card uses the following options within a valid DHCP response to define its TCP/IP settings. All of these options except the first are described in **RFC2132**.

- **IP Address** (from the **yiaddr** field of the DHCP response, described in **RFC2131)**: The IP address that the DHCP server is leasing to the cooling unit.
- **Subnet Mask** (option 1): The Subnet Mask value that the cooling unit needs to operate on the network.
- **Router,** i.e., Default Gateway (option 3): The default gateway address that the cooling unit needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the cooling unit.
- **Renewal Time, T1** (option 58): The time that the cooling unit must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): The time that the cooling unit must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other options. The cooling unit also uses the following options within a valid DHCP response. All of these options except the last are described in **RFC2132**.

- **Network Time Protocol Servers** (option 42): Up to two NTP servers (primary and secondary) that the cooling unit can use.
- **Time Offset** (option 2): The offset of the cooling unit's subnet, in seconds, from Coordinated Universal Time (UTC).
- **Domain Name Server** (option 6): Up to two Domain Name System (DNS) servers (primary and secondary) that the cooling unit can use.
- **Host Name** (option 12): The host name that the cooling unit will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the cooling unit will use (64-character maximum length).
- **Boot File Name** (from the **file** field of the DHCP response, described in **RFC2131**): The fully qualified directory-path to an APC user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the cooling unit will download the .ini file. After the download, the cooling unit uses the .ini file as a boot file to reconfigure its settings.

Port speed

The **Port Speed** setting defines the communication speed of the TCP/IP port.

- For **Auto-negotiation** (the default), Ethernet devices negotiate to transmit at the highest possible speed, but if the supported speeds of two devices are unmatched, the slower speed is used.
- Alternatively, you can choose either 10 Mbps or 100 Mbps, each with the option of half-duplex (for communication in only one direction at a time) or full-duplex (for communication simultaneously in both directions on the same channel).

DNS (Adminstration>Network>DNS>servers)

Use the options under **DNS** on the left navigation menu to configure and test the Domain Name System (DNS):

- Select **servers** to specify the IP addresses of the primary and optional secondary Domain Name System server. The cooling unit cannot send any e-mail messages unless at least the IP address of the primary DNS server is defined.
  - The cooling unit waits a maximum of 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the cooling unit does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the cooling unit or on a nearby segment (but not across a wide-area network [WAN]).
  - After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for that computer.
- Select **naming** to define the host name and domain name of the cooling unit:
  - **Host Name**: When an Administrator configures a host name here and a domain name in the **Domain Name** field, users can then enter a host name in any field in the cooling unit interface (except e-mail addresses) that accepts a domain name as input.
  - **Domain Name**: An Administrator must configure the domain name here only. In all other fields in the cooling unit interface (except e-mail addresses) that accept domain names, the cooling unit adds this domain name when only a host name is entered.
    - To override all instances of the expansion of a specified host name by the addition of the domain name, set the domain name field to its default, `example.com`, or to `0.0.0.0`.
    - To override the expansion of a specific host name entry—for example when defining a trap receiver—include a trailing period. The cooling unit recognizes a host name with a trailing period (such as *`mySnmpServer.`*) as if it were a fully qualified domain name and does not append the domain name.
- Select **test** to send a DNS query that tests the setup of your DNS servers:
  - As **Query Type**, select the method to use for the DNS query:
    - **by Host**: the URL name of the server
    - **by FQDN**: the fully qualified domain name
    - **by IP**: the IP address of the server
    - **by MX**: the Mail Exchange used by the server
  - In the **Query Question** field, identify the value to be used for the selected query type:

Query Type Selected	**Query Question to Use**
by Host	the URL
by FQDN	the fully qualified domain name, formatted as *`my_server.my_domain`*`.com`.
by IP	the IP address
by MX	the Mail Exchange address

  - View the result of the test DNS request in the **Last Query Response** field.

Web

Use the options under **Web** on the left navigation menu to configure the following:

Option	Description

access	To activate changes to any of the following access selections, log off from and back on to the cooling unit:
	• **Disable**: Disables all access to the Web interface. (You must use the control console to re-enable access to the Web interface. Select **Network** and **Web/SSL/TLS**. Then for HTTP access, select **Access** and **Enabled**, and for HTTPS access, also select **Web/SSL** and **Enabled**.)
	• **Enable HTTP** (the default): Enables Hypertext Transfer Protocol (HTTP), which provides Web access by user name and password, but does not encrypt user names, passwords, and data during transmission.
	• **Enable HTTPS**: Enables Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) to provide Web access. Secure Sockets Layer (SSL) encrypts user names, passwords, and data during transmission, and provides authentication of the cooling unit by digital certificate.
	See “Creating and Installing Digital Certificates” in the *Security Handbook* on the *Utility* CD to choose among the several methods for using digital certificates.
	When HTTPS is enabled, your browser displays a lock icon, usually at the bottom of the screen:
	HTTP Port: Identifies the TCP/IP port used for communication by HTTP with the cooling unit. The default is 80.
	HTTPS Port: Identifies the TCP/IP port used for communication by HTTPS with the cooling unit. The default is 443.
	You can change either port setting to the number of any unused port from 5000 to 32768 to enhance the protection provided by User Name and Password settings. You must then use a colon (:) in the address field of the browser to specify the non-default port number. For example, for port 5000 and the cooling unit IP address of 152.214.12.114, you would use one of these Web addresses:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

ssl cipher suites	Enable or disable any of the SSL encryption ciphers and hash algorithms: • **DES**: A block cipher that provides authentication by Secure Hash Algorithm. • **RC4_MD5** (enabled by default): A stream cipher, providing authentication by MD5 hash algorithm. • **RC4_SHA** (enabled by default): A stream cipher that provides authentication by Secure Hash Algorithm. • **3DES**: A block cipher that provides authentication by Secure Hash Algorithm.

Option	Description
ssl certificate	Add, replace, or remove a security certificate. **Status**: • **Not installed**: A certificate is not installed, or a certificate was installed by FTP or SCP to an incorrect location. Using **Add or Replace Certificate File** installs the certificate to the correct location, **/sec** on the cooling unit. • **Generating**: The cooling unit is generating a certificate because no valid certificate was found. • **Loading**: A certificate is being activated on the cooling unit. • **Valid certificate**: A valid certificate was installed or was generated by the cooling unit. Click on this link to view the certificate's contents. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the cooling unit generates a default certificate, a process which delays access to the interface for up to five minutes.** You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on. **Add or Replace Certificate File**: Enter or browse to the certificate file created with the Security Wizard. See "Creating and Installing Digital Certificates" in the *Security Handbook* on the *Utility* CD to choose a method for using digital certificates, including certificates created by the Security Wizard or generated by the cooling unit. **Remove**: Delete the current certificate.

Console

Use the options under **Console** on the left navigation menu to configure the following:

Option	Description

access	Choose one of the following:
	• **Disable**: Disables all access to the control console.
	• **Enable Telnet** (the default setting): Telnet transmits user names, passwords, and data without encryption.
	• **Enable SSH v1/v2**: Do not enable both versions 1 and 2 of Secure SHell (SSH) unless you require that both be activated at the same time. (Security protocols use extensive processing power.)
	• **Enable SSH v1 only**: Secure SHell (SSH) version 1 transmits user names, passwords, and data in encrypted form. There is little or no delay as you log on.
	• **Enable SSH v2 only**: Secure SHell (SSH) version 2 transmits user names, passwords, and data in encrypted form with somewhat more protection than version 1 from attempts to intercept, forge, or alter data during transmission. There is a noticeable delay as you log on.
	Identify the TCP/IP port used for communications with the cooling unit by Telnet and Secure SHell (SSH).
	• **Telnet Port**: The default is 23.
	• **SSH Port**: The default is 22.
	You can change the Port setting to the number of any unused port from 5000 to 32768 to enhance the protection provided by User Name and Password settings.
	• For Telnet, you must use either a colon (:) or a space in the command line, according to the requirements of your Telnet client program, to specify the non-default port number. For example, for a port number of 5000 and the cooling unit IP address of 152.214.12.114, your Telnet client requires one of the following commands:
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• For SSH, see the documentation for your SSH client for the command line format required to specify a non-default port when starting SSH.

ssh encryption	Enable or disable encryption algorithms (block ciphers) compatible with SSH version 1 or version 2 clients: SSH v1 algorithms: • **DES** • **Blowfish**: If your SSH v1 client cannot use Blowfish, which is always enabled, you must also enable DES. SSH v2 algorithms: • **3DES**: (enabled by default) • **Blowfish**: (enabled by default) • **AES 128** • **AES 256** Your SSH v2 client selects the enabled algorithm that provides the highest security. If your SSH client cannot use the default algorithms, you must enable an AES algorithm that it can use.

Option	Description
ssh host key	**Status** indicates the status of the host key (private key): • **SSH Disabled: No host key in use:** SSH is disabled and is not using a host key even if one is loaded. • **Generating**: The cooling unit is creating a host key because no valid host key was found. • **Loading**: A host key is being activated on the cooling unit. • **Valid**: One of the following valid host keys is in the **/sec** directory (the required location on the cooling unit): • A 1024-bit host key created by the APC Security Wizard. • A 768-bit RSA host key generated by the cooling unit. **Add or Replace**: Upload a host key file created by the APC Security Wizard to the **/sec** directory: 1. Click **Browse**. 2. Locate the file. 3. Click **Apply**. If you use FTP or Secure CoPy (SCP) instead to transfer the host key file, you must specify the **/sec** directory as the target location in the command. To use the APC Security Wizard, see the *Security Handbook* on the *Utility* CD. **Note:** To reduce the time required to enable SSH, create and upload a host key in advance. **If you enable SSH with no host key loaded, the cooling unit takes up to 5 minutes to create a host key, and the SSH server is not accessible during that time.** **Remove**: Remove the current host key.

Note: To use SSH, you must have a SSH client installed. Most Linux and other UNIX® platforms include a SSH client, but Microsoft Windows operating systems do not. SSH clients are available from various vendors.

SNMP

SNMPv1. All user names, passwords, and community names for SNMP are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMP access or set the access for each community to Read. (A community with Read access can receive status information and use SNMP traps.)

When using InfraStruXure Central to manage a cooling unit on the public network of a system, you must have SNMP enabled in the cooling unit. Read access will allow InfraStruXure Central to receive traps from the cooling unit, but Write access is required while you use the interface of the cooling unit to set InfraStruXure Central as a trap receiver.

For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available on the *Utility* CD or from the APC Web site, **www.apc.com**.

Use the options under **SNMP** on the left navigation menu to configure the following:

Option	**Description**
access	**Enable SNMPv1 Access:** Enables SNMP version 1 as a method of communication with this device.
access control	You can configure up to four access control entries to specify which Network Management Systems (NMS) have access to this device. The opening page for access control, by default, assigns one entry to each of the four available SNMPv1 communities, but you can edit these settings to apply more than one entry to any community to grant access by several specific IP addresses, host names, or IP address masks. To edit the access control settings for a community, click its community name. • If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network. • If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device. **Community Name:** The name that a NMS must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are "public", "private", "public2", and "private2". **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain **255** restrict access as follows: • 149.225.12.**255**: Access only by a NMS on the 149.225.12 segment. • 149.225.**255**.**255**: Access only by a NMS on the 149.225 segment. • 149.**255**.**255**.**255**: Access only by a NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as **255**.**255**.**255**.**255**: Access by any NMS on any segment. **Access Type**: The actions a NMS can perform through the community. • **Read**: GETS only, at any time. • **Write**: GETS at any time, and SETS when no user is logged onto the Web interface or control console. • **Write+**: GETS and SETS at any time. • **Disabled**: No GETS or SETS at any time.

SNMPv3. For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users. An SNMPv3 user must have a user profile assigned in the MIB software program to perform GETs and SETs, browse the MIB, and receive traps.

Note: To use SNMPv3, you must have a MIB program that supports SNMPv3.
Note: The cooling unit supports only MD5 authentication and DES encryption.

Option	Description
access	**SNMPv3 Access:** Enables SNMPv3 as a method of communication with this device.
user profiles	By default, lists the settings of four user profiles, configured with the user names "apc snmp profile1" through "apc snmp profile 4", and no authentication and no privacy (no encryption of data). To edit the following settings for a user profile, click a user name in the list. **User Name:** The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters. **Authentication Passphrase:** A phrase of 15 to 32 ASCII characters that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time. **Privacy Passphrase:** A phrase of 15 to 32 ASCII characters that ensures the privacy of the data (by means of encryption) that a NMS is sending to this device or receiving from this device through SNMP v3. **Authentication Protocol**: The APC implementation of SNMPv3 supports MD5 authentication. Authentication will not occur unless MD5 is selected here. **Privacy Protocol:** The APC implementation of SNMPv3 supports DES as the protocol for encrypting and decrypting data. Privacy of transmitted data requires that DES is selected here. **Note:** You cannot select the privacy protocol if no authentication protocol is selected.

Option	Description
access control	You can configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles, but you can edit these settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks. • If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device. • If you configure multiple access entries for one user profile, the limit of four entries requires that one or more of the other user profiles must have no access control entry. If no access control entry is listed for a user profile, no NMS that uses that profile has any access to this device. To edit the access control settings for a user profile, click its user name. **Access:** Mark the **Enable** checkbox to activate the access control specified by the parameters in this access control entry. **User Name:** Select from the drop-down list the user profile to which this access control entry will apply. The choices available are the four user names that you configure through the "user profiles" option on the left navigation menu. **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows: • 149.225.12.**255**: Access only by a NMS on the 149.225.12 segment. • 149.225.**255**.**255**: Access only by a NMS on the 149.225 segment. • 149.**255**.**255**.**255**: Access only by a NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as **255**.**255**.**255**.**255**: Access by any NMS on any segment.

FTP server

The **FTP server** settings enable (by default) or disable access to the FTP server and specify the TCP/IP port (21 by default) that the FTP server uses for communication with the cooling unit. The FTP server uses both the specified port and the port one number lower than the specified port.

You can change the **Port** setting to the number of any unused port from 5000 to 32767 to enhance the protection provided by User Name and Password settings. You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 5001 and the cooling unit IP address of 152.214.12.114, you would use this command:

```
ftp 152.214.12.114:5001
```

Note: FTP transfers files without encryption. For higher security, disable the FTP server, and transfer files with Secure CoPy (SCP). Selecting and configuring Secure SHell (SSH) enables SCP automatically.

Note: At any time that you want the cooling unit to be accessible for management by InfraStruXure Central, FTP Server must be enabled in the cooling unit interface.

Related Topics

See these related topics:

- "Console" on this page to configure SSH.
- "How to use FTP or SCP to retrieve the log files" on page 30 to obtain a text version of the event log.

Administration: Notification

Event Actions

Types of notification

You can configure event actions to occur in response to an event or a group of events. These actions notify users of the event in any of several ways:

- Active, automatic notification. The specified users or monitoring devices are contacted directly.
  - – E-mail notification
  - – SNMP traps
  - – Syslog notification

  To set up additional methods of active notification that are not included in the **Event Action** options, see “Configuration” on page 23 for information on configuring the output contact.

- Indirect notification through the event log. If none of the direct notification methods are configured, users must check the log to determine which events have occurred.

  Another method of indirect notification, not included in the **Event Action** options, is the use of informational queries. See “access control” on page 46, under “SNMP” , for a description of SNMP access types that enable a Network Management System (NMS) to perform informational queries. Configuring the most restrictive SNMP access type, READ, or using Serial Modbus enables informational queries without the risk of allowing remote configuration changes.

Configuring event actions

You can configure event actions for individual events or for predefined groups of events.

Configuring by event. To define event actions for an individual event:

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.
2. Follow the on-screen instructions to list events by severity, either by main category or sub-category.
3. In the list of events, check the marked columns to see whether the action you want is already configured for the event. (By default, logging is configured for all events.)
4. For details of the current configuration, such as the recipients to be notified by e-mail or the Network Management Systems (NMSs) to be notified by SNMP traps, click on the event name.
5. Add to or change the event configuration.

   Note: A Syslog server must be configured before you can display or use the Syslog option, and at least one e-mail recipient or trap receiver must be configured before you can display or use the detailed e-mail and trap notification options.

   – Mark the checkboxes to enable (or clear them to disable) event logging or Syslog for this event.

– Click on any e-mail recipient or trap receiver, and specify any value up to three digits to configure the following detailed options:

  - How long, in seconds or minutes, the cooling unit waits after the event occurs before sending e-mail to the selected e-mail recipient or a trap to the selected trap receiver. If the event clears during this delay period, no notification is sent. To configure a delay longer than 999 seconds (16 minutes, 39 seconds), use minutes.
  - How frequently to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. E-mail or a trap repeats at the time interval specified here in seconds, minutes, or hours, unless the event has cleared.
  - The number of times to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. Choose to send e-mail or a trap a specified number of times or to repeat the notification an unlimited number of times. In either case, notification stops if the event clears.

When configuring events, you can enable or disable notification to configured e-mail recipients, Syslog servers, or trap receivers, but you cannot add or remove any recipients, receivers, or Syslog servers. To add or remove recipients, receivers, or servers, see “Syslog” on page 27, “E-mail recipients” on page 53, and “Trap receivers.” on page 54

Configuring by group. To configure a group of events simultaneously:

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by group** under **Event Actions** on the left navigation menu.
2. Choose how you want events to be grouped for configuration and select **Next**:
   – If you choose **Events by severity**, you can then select all events of one or more severity types.

   Note: When configuring events by severity, you must use their existing severity. You cannot change the severity of an event.

   – If you choose **Events by category**, you can then select all events in one or more predefined categories.
3. Select event actions for all events in the group.

   Note: A Syslog server must be configured in order to display or use the Syslog option, and at least one e-mail recipient (for e-mail notification) or at least one trap receiver (for notification by SNMP traps) must be configured in order to display the detailed e-mail and trap receiver notification options.

   – Click the **Logging** button to choose logging for all events in the group. Click **Next>>**, and then mark the checkboxes to enable (or clear them to disable) event logging or Syslog for these events.

   – Click the **E-mail Recipients** or **Trap Receivers** button, click **Next>>**, and select an e-mail recipient or trap receiver. Then specify any value up to three digits to configure the following detailed options:

   - How long, in seconds or minutes, the cooling unit waits after one of these events occurs before sending e-mail to the selected e-mail recipient or a trap to the selected trap receiver. If the event clears during this delay period, no notification is sent. To configure a delay longer than 999 seconds (16 minutes, 39 seconds), use minutes.
   - How frequently to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. E-mail or a trap repeats at the time interval specified here in seconds, minutes, or hours, unless the event has cleared.
   - The number of times to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. Choose to send e-mail or a trap a specified number of times or to repeat the notification an unlimited number of times. In either case, notification stops if the event clears.

   To add or remove recipients or receivers, see “E-mail recipients” on page 53 or “Trap receivers.” on page 54
4. Click **Next>>**, and then click **Apply** to confirm the displayed selections.
5. Click **Finish** to return to the **by group** page, or select **Configure Additional Actions** to keep the selected event group and to configure the remaining **Logging**, **E-mail Recipients**, or **Trap Receivers** actions for this group.

Active, Automatic, Direct Notification

E-mail notification

Overview of setup. Use the Simple Mail Transfer Protocol (SMTP) to send e-mail to up to four recipients when an event occurs.

To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and, optionally, of the secondary Domain Name System (DNS) servers

  See “DNS (Adminstration>Network>DNS>servers)” on page 41.

- The IP address or DNS name for **SMTP Server** and the **From Address** setting for SMTP

  See “SMTP (Administration>Notification>E-mail>server)” on page 53.

- The e-mail addresses for a maximum of four recipients

  To configure recipients, see “E-mail recipients” on page 53.

Note: You can use the **To Address** setting of the **recipients** option to send e-mail to a text-based pager.

SMTP (Administration>Notification>E-mail>server). Use this option to define the following settings:

Setting	Description
Local SMTP Server	The IP address (or if DNS is configured, the DNS name) of the local SMTP server. **Note:** This definition is required only when **SMTP Server** is set to **Local** when E-mail recipients are being configured. See "E-mail recipients" on page 53.
From Address	The contents of the **From** field in the format *user@* [*IP_address*] (if an IP address is specified as **Local SMTP Server**) or *user@domain*.com (if DNS is configured and the DNS name is specified as **Local SMTP Server**) in the e-mail messages sent by the cooling unit. **Note:** The local SMTP server's configuration may require that you use a valid user account on the server for this setting. See the server's documentation for more information.

E-mail recipients. Use this option to identify up to four e-mail recipients. Click a recipient **To Address** to edit that configuration. Select **Add Recipient** to add a new recipient.

Setting	Description
To Address	Defines the user and domain names of the recipient. To use e-mail for paging, use the e-mail address for that recipient's pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page. You can bypass the DNS lookup of the mail server's IP address by using the IP address in brackets instead of the e-mail domain name. For example, use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly. **Note:** The recipient's pager must be able to use text-based messaging.
E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.
SMTP Server	Selects one of the following methods for routing e-mail: • **Local**: Through the SMTP server of the cooling unit (the recommended setting). This option ensures that the e-mail is sent before the cooling unit's 20-second time-out, and, if necessary, is retried several times. Also do one of the following: • Enable forwarding at the cooling unit's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Always check with the administrator of your SMTP server before changing its configuration to allow forwarding. • Set up a special e-mail account for the cooling unit to forward e-mail to an external mail account. • **Recipient**: Directly to the recipient's SMTP server. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent because, with this option, the cooling unit tries to send the e-mail only once. When the recipient uses the cooling unit's SMTP server, this setting has no effect.
Format	Select **Long** or **Short**. The **Long** format contains Name, Location, Contact, IP address, serial number of the device, date, time, event code, and event description. The **Short** format provides only the event description.

E-mail test. Use this option to send a test message to a configured recipient.

SNMP traps

Trap receivers. View trap receivers by NMS IP/Host Name. You can configure up to six trap receivers.

- To open the page for configuring a new trap receiver, click **Add Trap Receiver**.
- To modify or delete a trap receiver, first click its IP address or host name to access its settings. (If you delete a trap receiver, all notification settings configured under Event Actions for the deleted trap receiver are set to their default values.)
- To specify the trap type for a trap receiver, select either the SNMPv1 or SNMPv3 radio button. For a NMS to receive both types of traps, you must configure two trap receivers for that NMS, one for each trap type.

Item	Definition
Trap Generation	Enable (the default) or disable trap generation for this trap receiver.
NMS IP/Host Name	The IP address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.

SNMPv1 option.

Community Name	The name ("public" by default) used as an identifier when SNMPv1 traps are sent to this trap receiver.
Authenticate Traps	When this option is enabled (the default), the NMS identified by the NMS IP/ Host Name setting will receive authentication traps (traps generated by invalid attempts to log on to this device). To disable that ability, clear the checkbox.

SNMPv3 option. Select the identifier of the user profile for this trap receiver. (To view the settings of the user profiles identified by the user names selectable here, choose **Network** on the top menu bar and **user profiles** under **SNMPv3** on the left navigation menu.)

SNMP trap test. Use this option to test the sending of a trap to a configured trap receiver.

Last Test Result—The result of the most recent SNMP trap test. A successful SNMP trap test verifies only that a trap was sent; it does not verify that the trap was received by the selected trap receiver. A trap test succeeds if all of the following are true:

- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver is enabled.
- If a host name is selected for the **To** address, that host name can be mapped to a valid IP address.

To—Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver was ever configured, a link to the **Trap Receiver** configuration page is displayed. (If a trap receiver was deleted, or was reset to its default values by this or any other management application, the default values for its trap type are listed.)

Administration: General Options

Information about the Cooling Unit

Identification

Use this option to define the System **Name**, **Contact**, and **Location** values used to identify the cooling unit. For example, you might configure **Name** as Test Lab, **Contact** (whom to contact about the device) as Donald Adams, and **Location** as Building 3.

Date & time

Mode. Use this option to set the time and date used by the cooling unit. The option displays the current settings, and allows you to change those settings manually or through a Network Time Protocol (NTP) Server.

- **Manual**: Use this selection to do one of the following:
  - Enter the date and time for the cooling unit
  - Mark the checkbox **Apply Local Computer Time** to match the date and time settings of the computer you are using, and click **Apply**.
- **Synchronize with NTP Server**: Use this selection to have an NTP Server define the date and time for the cooling unit.

Setting	Definition
Primary NTP Server	Enter the IP address or domain name of the primary NTP server.
Secondary NTP Server	Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.
Time Zone	Select a time zone. The number of hours preceding each time zone in the list is the offset from UTC (Coordinated Universal Time, Temps Universel Coordonné, formerly Greenwich Mean Time), the international time standard.
Update Interval	Define how often, in hours, the cooling unit accesses the NTP Server for an update. The minimum is 1 hour; the maximum is 8760 hours (1 year).
Update Using NTP Now	Mark this checkbox and click **Apply** to initiate an immediate update of the date and time by the NTP Server.

Enable and configure Daylight Saving Time. Use this option to enable either traditional United States Daylight Saving Time (DST) or to enable and configure a customized daylight saving time, with starting and ending dates and time that you specify to match how Daylight Saving Time is implemented in your local area. DST is disabled by default.

When customizing Daylight Saving Time:

- If the local Daylight Saving Time always starts or ends on the 4th occurrence of a specific weekday of a month (for example, the 4th Sunday), choose Fourth/Last. If a 5th Sunday occurs in that month in a subsequent year, the time setting will still change to or from Daylight Saving Time on the 4th Sunday.
- If the local Daylight Saving Time always starts or ends on the last occurrence of a specific weekday of a month, such as the last Sunday of that month, regardless of whether that last Sunday is the 4th or the 5th Sunday, choose Fifth/Last.

Selecting a date format. Select the numerical format in which to display all dates in this User Interface. In the selections, each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.

User configuration file (ini)

As an Administrator, you can retrieve a dynamically generated .ini file of the current configuration of the cooling unit and export that file to another cooling unit or to multiple cooling units.

Use the **Browse** button to upload an .ini file.

For further detail, see “How to Export Configuration Settings” on page 62.

Unit preference

Event Log Color Coding . Enable/Disable

Select the temperature scale (Fahrenheit or Celsius) in which to display all temperature measurements in this user interface.

Temperature Scale . Fahrenheit/Celsius

Note: Changing the temperature scale will also change other unit settings between Metric and English. Settings that will be affected include flow rates and pressure measurements.

Reset the interface

Use the **Reset/Reboot** option to perform any of the following actions:

Action	Definition
Reboot Management Interface	Restarts the management interface of the device without turning off and restarting the device itself.
Reset All	Resets Security, Network, Notification, General, and Logs configuration settings. It does not reset Cooling Group and Cooling Unit configuration settings. Mark the **Include TCP/IP** checkbox to include the setting that determines how this device must obtain its TCP/IP settings. That setting will be reset to its default, DHCP & BOOTP. **Note:** To reset all device settings except the TCP/IP settings, leave the **Include TCP/IP** checkbox unchecked.
Reset Only	You can choose one or more of the following options by marking their checkboxes: **TCP/IP**: Resets only the setting that determines how this device must obtain its TCP/IP settings. That setting will be reset to its default, DHCP & BOOTP. **Event Configuration**: Resets only events to their default configuration. Any configuration changes, by event or by group, will revert to their default settings.

Serial Modbus

To configure Modbus, select the **Administration** tab, **General** on the top menu bar, and **Serial Modbus** on the left navigation menu. You can enable or disable Modbus, choose a baud rate, and specify a unique identifier.

Modbus defines a request/response message structure for a client/server environment. The APC implementation of Modbus uses Remote Terminal Unit (RTU) mode. You can use Modbus to view the cooling unit through your building management system interface. It is read-only.

- The Modbus interface supports 3-wire RS-485 (D0, D1, and Ground).
- Modbus runs at 9600 or 19200 bps.

The Modbus register map for the cooling unit defines the data (type, location, and valid responses) available through Modbus. To download the latest Modbus register map, go to the APC Web site (**www.apc.com**), search by product, and click the documentation link. Click on the link to the register map in the list of documentation. Check the publication date at the start of the file.

For more information on Modbus, see the Modbus Standard Library at **www.modbus.org**.

Quick links

Select the **Administration** tab, the **General** option on the top menu bar, and the **Quick Links** option on the left navigation menu to view the three URL links displayed at the bottom left of each page of the interface.

By default, these links access the following Web pages:

- **APC's Web Site**: The APC home page.
- **Testdrive Demo**: A demonstration page where you can use samples of APC Web-enabled products.
- **APC Monitoring**: The home page of the APC Remote Monitoring Service.

To reconfigure a link, click on that link in the **Display** column, and change any of the following:

- **Display**: The short link name displayed on each interface page.
- **Name**: A name that fully identifies the target or purpose of the link.
- **Address**: Any URL — for example the URL of another device and server.

About

The hardware information is especially useful to APC Customer Support in helping to troubleshoot problems with your cooling unit. The serial number and MAC address accessible through the **About** menu option are also available on the cooling unit itself. Management Uptime shows the time that has elapsed since the last reset or reboot.

Firmware information, listed under Application Module and APC OS (AOS), indicates the name, firmware version number, and the date and time each firmware module was created. This information may also be useful in troubleshooting and enables you to determine quickly if updated firmware is available to download from the APC Web site.

- Hardware Factory
    - Model Number
    - Serial Number
    - Hardware Revision
    - Manufacture Date
    - MAC Address
    - Management Uptime
- Application Module
    - Name
    - Version
    - Date
    - Time
- APC OS (AOS)
    - Name
    - Version
    - Date
    - Time

APC Device IP Configuration Wizard

Capabilities, Requirements, and Installation

Use the Wizard to configure basic TCP/IP settings

The APC Device IP Configuration Wizard configures the IP address, subnet mask, and default gateway of one or more cooling units. You can use the Wizard the following ways:

- Automatically discover and configure unconfigured cooling units remotely over your TCP/IP network.
- Configure or reconfigure a cooling unit through a direct connection from the serial port of your computer to the device that contains the card.

Note: The cooling units must be on the same network segment as the computer that is running the Wizard.

System requirements

The Wizard runs on Microsoft Windows 2000, Windows Server 2003, and Windows XP operating systems.

Installation

To install the Wizard from the *Utility* CD:

1. If autorun is enabled, the user interface of the CD starts when you insert the CD. Otherwise, open the file **contents.htm** on the CD.
2. Click on the **Device IP Configuration Wizard** and follow the instructions.

To install the Wizard from a downloaded executable file:

1. Go to **www.apc/tools/download**.
2. Download the Device IP Configuration Wizard
3. Run the executable file in the folder to which you downloaded it.

Use the Wizard

Note: Most software firewalls must be temporarily disabled for the Wizard to discover unconfigured cooling units.

Launch the Wizard

The installation creates a shortcut link in the **Start** menu to launch the Wizard.

Configure the basic TCP/IP settings remotely

Prepare to configure the settings. Before you run the Wizard:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. If you are configuring multiple unconfigured cooling units, obtain the MAC address of each one to identify it when the Wizard discovers it. (The Wizard displays the MAC address on the screen on which you then enter the TCP/IP settings.)

- For a Network Management Card that you install in the cooling unit, the MAC address is on a label on the back of the card.
- The MAC address is on a label in the cooling unit's electrical cabinet.
- You can also obtain the MAC address from the Quality Assurance slip that came with the cooling unit.

Run the Wizard to perform the configuration. To discover and configure, over the network, cooling units that are not configured:

1. From the **Start** menu, launch the Wizard. The Wizard automatically detects the first cooling unit that is not configured.
2. Select **Remotely (over the network)**, and click **Next >**.
3. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the unconfigured cooling unit identified by the MAC address at the top of the screen. Then click **Next >**.

   On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the cooling unit after you transmit the settings.
4. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
5. The Wizard searches for another unconfigured cooling unit or device. If it finds one, it displays the screen with data entry boxes for the TCP/IP settings of that cooling unit.
   - To skip configuring the cooling unit or device whose MAC address is currently displayed, click **Cancel**.
   - To configure the TCP/IP settings of the next card, repeat this procedure beginning at step 3.

Configure or reconfigure the TCP/IP settings locally

To configure a single cooling unit through a serial connection:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the provided serial configuration cable from an available communications port on your computer to the serial port of the cooling unit. Make sure no other device is using the computer port.
3. From the **Start** menu, launch the Wizard application.
   a. If the cooling unit is not configured, wait for the Wizard to detect it.
   b. If you are assigning basic TCP/IP settings serially to a cooling unit, click **Next>**.
4. Select **Locally (through the serial port)**, and click **Next >**.
5. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the cooling unit. Then click **Next >**.
6. On the **Transmit Current Settings Locally** screen, if you select **Start a Web browser when finished**, the default Web browser connects to the cooling unit after the Wizard transmits the settings.
7. Switch the main breaker on the front of the electrical panel to OFF. Wait one second. Switch the main breaker to ON.

   Note: If you wait too long to return power to the cooling unit, you must repeat step 7.

   If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
8. If you selected **Start a Web browser when finished** in step 6, you can now configure other parameters through the Web interface of the cooling unit.

How to Export Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

An Administrator can retrieve the .ini file of the cooling unit and export that file to another cooling unit or to multiple cooling units.

1. Configure the cooling unit to have the settings you want to export.
2. Retrieve the .ini file from that cooling unit.
3. Customize the .ini file (to change at least the TCP/IP settings) and make a copy to export.
4. Use a file transfer protocol supported by the cooling unit to transfer the copied file to one or more additional cooling units. (To transfer the file to multiple cooling units simultaneously, use an FTP or SCP script or the APC .ini file utility.

Each receiving cooling unit uses the file to reconfigure its own settings, and then deletes it.

Contents of the .ini file

The config.ini file that you retrieve from the cooling unit contains the following:

- *Section headings*, which are category names enclosed in brackets ([ ]), and under each section heading, *keywords,* which are labels describing specific cooling unit settings.

  Note: Only section headings and keywords supported by the cooling unit from which you retrieve the file are included.

- Each keyword is followed by an equals sign and the current *value* for that parameter's setting, either the default value (if the value has not been specifically configured) or the configured value.
  – The `Override` keyword, with its default value, prevents one or more keywords and their device-specific values from being exported. For example, in the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the cooling unit) blocks the exporting of the values for the keywords `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.
  – You must edit the section `[SystemDate/Time]` to set the system date and time of a receiving cooling unit or cause that cooling unit to use an NTP Server to set its date and time.

  See "Customizing" on page 63 for configuration guidelines for date and time settings.

Detailed procedures

Use the following procedures to retrieve the settings of one cooling unit and export them to one or more cooling units.

Retrieving. To set up and retrieve an .ini file to export:

1. Configure the cooling unit with the settings you want to export.

   Note: To avoid errors, configure the cooling unit by using its user interface whenever possible. Directly editing the .ini file risks introducing errors.

2. Use FTP to retrieve the file config.ini from the cooling unit you configured:

   a. Open a connection to the cooling unit, using its IP Address. For example:

   ```
   ftp> open 158.165.2.132
   ```

   b. Log on, using the Administrator user name and password configured for the cooling unit.

   c. Retrieve the config.ini file containing the cooling unit's current settings:

   ```
   ftp> get config.ini
   ```

   The file is written to the folder from which you launched FTP.

   To create batch files and use an APC utility to retrieve configuration settings from multiple cooling units and export them to other cooling units, see *Release Notes: ini File Utility, version 1.0* on the *Utility* CD.

Customizing. You must customize the file to change at least the TCP/IP settings before you export it.

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   - To define values, opening and closing quotation marks are optional, except to enclose values that contain leading or trailing spaces or values which are already enclosed in quotation marks. (Leading or trailing spaces not within the opening and closing quotation marks are ignored.)
   - To export a specific system date and time or any scheduled events, you must configure the values directly in the .ini file.
     - To export a specific system time, export only the configured `[SystemDate/Time]` section as a separate .ini file. (The time necessary to export a large file would cause the configured time to be significantly inaccurate.)
     - For greater accuracy, if the cooling units receiving the file can access a Network Time Protocol (NTP) Server, set the value for the `NTPEnable` keyword as follows: `NTPEnable=enabled`
   - Add comments about changes that you made. The first printable character of a comment line must be a semicolon (`;`).
2. Copy the customized file to another file name in the same folder:
   - The copy, which you will export to other cooling units, can have any file name up to 64 characters and must have the .ini file suffix.
   - Retain the original customized file for future use. **The file that you retain is the only record of your comments.** They are removed automatically from the file that you export.

Transferring the file to a single cooling unit. To transfer the .ini file to one other cooling unit, do either of the following:

- From the Web interface of the receiving cooling unit, select the **Administration** tab, **General** on the top menu bar, and **User Config File** on the left navigation menu. Enter the full path of the .ini file to transfer or use the **Browse** button to identify the location of the .ini file.
- Use any of the file transfer protocols supported by cooling units (including FTP, FTP Client, SCP, and TFTP). The following example uses FTP:
  a. From the folder containing the customized .ini file and its copy, use FTP to log in to the cooling unit to which you are exporting the .ini file. For example:

  ```
  ftp> open 158.165.4.135
  ```

  b. Export the copy of the customized .ini file. The receiving cooling unit accepts any file name that has the .ini suffix, is no more than 64 characters in length, and is exported to its root directory.

  ```
  ftp> put filename.ini
  ```

Exporting the file to multiple cooling units. T

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single cooling unit.
- Use a batch processing file and the APC .ini file utility.

  To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* on the *Utility* CD.

The Upload Event and Error Messages

The event and its error messages

The following event occurs when the receiving cooling unit completes using the .ini file to update its settings.

```
Configuration file upload complete, with number valid values
```

If a keyword, section name, or value is invalid, the event text is extended to include notification of the following errors.

Note: The export to and the subsequent upload by the receiving cooling unit succeeds even if there are errors.

Event text	Description
Configuration file warning: Invalid keyword on line *number.* Configuration file warning: Invalid value on line *number.*	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number.*	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number.*	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, the cooling unit stores and processes what it can, but ignores what it cannot. Reduce the size of the file, or divide it into two files, and try uploading again.

Errors generated by overridden values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values.

See "Contents of the .ini file" on page 62 for information about which values are overridden.

The overridden values are device-specific and not appropriate to export to other cooling units. Therefore, you can ignore these error messages. To prevent these error messages from occurring, you can delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Related Topics

On Windows operating systems, instead of using the preceding procedure for transferring .ini files, you can choose to update the basic TCP/IP settings of cooling units by using the APC Device IP Configuration Wizard.

See "APC Device IP Configuration Wizard" on page 59 for a detailed description of how to discover and configure the basic TCP/IP settings of unconfigured cooling units remotely over your TCP/IP network. This section will also tell you how to configure or reconfigure one cooling unit through a direct connection from the serial port of your computer to the cooling unit.

File Transfers

How to Upgrade Firmware

Benefits of upgrading firmware

Upgrading the firmware on the cooling unit has the following benefits:

- New firmware has the latest bug fixes and performance improvements.
- New features become available for immediate use.
- Keeping the firmware versions consistent across your network ensures that all cooling units support the same features in the same manner.

Firmware files

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module. Each module contains one or more Cyclical Redundancy Checks (CRCs) to protect its data from corruption during transfer.

The AOS and application module files used with the cooling unit share the same basic format:

`apc_`*`hardware-version_type_firmware-version`*`.bin`

- apc: Indicates that this is an APC file.
- *`hardware-version`*: `hw0`*`x`* identifies the version of the hardware on which you can use this binary file.
- *`type`*: `aos` if the file is the AOS module, or `acrp` if the file is the application module for the cooling unit.
- *`firmware-version`*: The version number of the file.
- `bin`: Indicates that this is a binary file.

Obtain the latest firmware version

Automated upgrade tool for Microsoft Windows systems. An upgrade tool automates the transferring of the firmware modules on any supported Windows operating system. Obtain the latest version of the tool at no cost from **www.apc.com/tools/download**. At this Web page, find the latest firmware release for your APC product and download the automated tool. Never use the tool for one APC product to upgrade the firmware of another product.

Manual upgrades, primarily for Linux systems. If computers on your network are running Linux, you must upgrade the firmware of the cooling units manually by using the separate APC firmware modules (AOS module and application module).

If you have a networked computer running a supported Microsoft Windows operating system on your network, you can use the tool described in “Automated upgrade tool for Microsoft Windows systems” on page 66 to upgrade the firmware of the cooling unit automatically over the network. This tool automates the entire upgrade process.

You can obtain the individual firmware modules you need for a manual firmware upgrade by extracting them from the automated tool.

To extract the firmware files:

1. Run the tool.
2. At the prompts, click **Next>**, and then specify the directory location to which the files will be extracted.
3. When the **Extraction Complete** message displays, close the dialog box.

Firmware file transfer methods

Use one of these methods to upgrade the firmware of the cooling unit:

- From a networked computer running a Microsoft Windows operating system, you can use the automated firmware upgrade tool on your CD or downloaded from the APC Web site.
- From a networked computer on any supported operating system, you can use FTP or SCP to transfer the individual AOS and application firmware modules.
- For the cooling unit that is not on your network, you can use XMODEM through a serial connection to transfer the individual AOS and application firmware modules from your computer to the cooling unit.

  Note: When you transfer individual firmware modules you must transfer the AOS module to the cooling unit before you transfer the application module.

Use FTP or SCP to upgrade one cooling unit

Instructions for using FTP. For you to be able to use FTP to upgrade a single cooling unit over the network:

- The cooling unit must be connected to the network.
- The FTP server must be enabled at the cooling unit.
- The cooling unit must have its TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway** addresses) configured.

To use FTP to upgrade the cooling unit:

1. Open an MS-DOS command prompt window on a computer that is connected to the network. Go to the directory that contains the firmware upgrade files, and list the files. For the directory `C:\apc`, the commands would be those shown in **bold**:

   ```
   C:\>cd\apc
   C:\apc>dir
   ```

   Files listed for the cooling unit, for example, might be the following (with *xxx* representing the version number of each file):

   ```
   –apc_hw03_aos_xxx.bin
   –apc_hw03_acrp_xxx.bin
   ```

2. Open an FTP client session:

   ```
   C:\apc>ftp
   ```

3. Type `open` and the cooling unit's IP address, and press ENTER. If the **port** setting for the FTP Server (accessible through the **Administration** tab, **Network** on the top menu bar, and **FTP Server** on the left navigation menu) has changed from its default of **21**, you must use the non-default value in the FTP command.
   - For some FTP clients, use a colon to add the port number to the end of the IP address.
   - For Windows FTP clients, separate the port number from the IP address by a space. For example, if the cooling unit's **FTP Server Port** setting has been changed from its default of **21**, such as to **21000**, you would use the following command for a Windows FTP client transferring a file to the cooling unit with an IP address of 150.250.6.10.
     `ftp>` **open 150.250.6.10 21000**
4. Log on using the Administrator user name and password. (**apc** is the default for both.)
5. Upgrade the AOS. In the `put` command in the following example, *xxx* is the firmware version number, with no periods separating the digits:

   ```
   ftp> bin
   ftp> put apc_hw03_aos_xxx.bin
   ```

6. When FTP confirms the transfer, type **quit** to close the session.
7. Wait 20 seconds, and then repeat step 2 through step 5, but in step 5, use the application module file name instead of the AOS module.

Instructions for using SCP. To use Secure CoPy (SCP) to upgrade the firmware for one cooling unit:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the cooling unit. The following example assumes a cooling unit's IP address of 158.205.6.185, and an AOS module of **apc_hw03_aos_*xxx*.bin**. (with *xxx* representing the version number of the AOS module, with no periods separating the digits).

   ```
   scp apc_hw03_aos_xxx.bin apc@158.205.6.185:apc_hw03_aos_xxx.bin
   ```

3. Use a similar SCP command line, with the name of the application module instead of the AOS module, to transfer the application module to the cooling unit.

Upgrade multiple cooling units

Export configuration settings. You can create batch files and use an APC utility to retrieve configuration settings from multiple cooling units and export them to other cooling units.

See *Release Notes: ini File Utility, version 1.0* on the *Utility* CD.

Use FTP or SCP to upgrade multiple cooling units. To upgrade multiple cooling units using an FTP client or using SCP, write a script which automatically performs the procedure. For FTP, use the steps in "Use FTP or SCP to upgrade one cooling unit" in the script.

Use XMODEM to upgrade one cooling unit

To use XMODEM to upgrade the firmware for a single cooling unit that is not on the network:

1. Obtain the individual firmware modules (the AOS module and the application module) from **www.apc.com/tools/download**.
2. Select a serial port at the local computer and disable any service which uses that port.
3. Connect the configuration cable (APC part number 940-0103) that came with the cooling unit to the selected port and to the serial port at the cooling unit.
4. Run a terminal program (such as HyperTerminal), and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control, and save the changes.
5. Press ENTER twice to display the **User Name** prompt.
6. Enter the Administrator user name and password (**apc** by default for both).
7. From the **Control Console** menu, select **System**, then **Tools**, then **File Transfer**, then **XMODEM**; and type `Yes` at the prompt to continue.
8. At the prompt for the baud rate, enter an appropriate baud rate for the terminal program to use for the transfer. A higher baud rate causes faster firmware upgrades.

   Note: Allowed values are 2400, 9600, 19200, and 38400. To choose a baud rate different from your current connection, disconnect from the terminal session. Configure the selected port for the desired baud rate and reconnect the terminal session.

Press ENTER. The screen displays uppercase C, indicating transfer mode.

9. From the terminal program's menu, select the binary AOS file to transfer via XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600 (if you selected a different rate in step 8). The cooling unit automatically restarts.

10. Repeat step 4 through step 9 to install the application module. In step 9, use the application module file name, not the AOS module file name.

For information about the file name format used for application modules, see "Firmware files" .

Verifying Upgrades and Updates

Overview

To verify that the firmware upgrade was successful, see the **Last Transfer Result** message, available through the **FTP Server** option of the **Network** menu (in the control console only), or use an SNMP GET to the **mfiletransferStatusLastTransferResult** object identifier (OID).

Last transfer result codes

Code	Description
Successful	The file transfer was successful.
Result not available	There are no recorded file transfers.
Failure unknown	The last file transfer failed for an unknown reason.
Server inaccessible	The TFTP or FTP server could not be found on the network.
Server access denied	The TFTP or FTP server denied access.
File not found	The TFTP or FTP server could not locate the requested file.
File type unknown	The file was downloaded but the contents were not recognized.
File corrupt	The file was downloaded but at least one Cyclical Redundancy Check (CRC) failed.

Use the Web interface to verify the versions of the upgraded AOS and application modules by selecting the **Administration** tab, **General** on the top menu bar, and **Factory Info** on the left navigation menu, or use an SNMP GET to the MIB II **sysDescr** OID.

APC Worldwide Customer Support

Customer support for this or any other APC product is available at no charge in any of the following ways:

- Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
  - **www.apc.com** (Corporate Headquarters)
    Connect to localized APC Web sites for specific countries, each of which provides customer support information.
  - **www.apc.com/support/**
    Global support searching APC Knowledge Base and using e-support.
- Contact the APC Customer Support Center by telephone or e-mail.
  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

For information on how to obtain local customer support, contact the APC representative or other distributors from whom you purchased your APC product.